Ideal Meeting Location According to User privacy

[1]Dipali D. Kosare
[1]Computer Science & Engineering,
RTMNU University, A.C.E
Wardha, Maharashtra, India
[1]deepalikosare@gmail.com

[2]Prof. D. M. Sable
[2]Computer Science & Engineering,
RTMNU University, A.C.E,
Wardha, Maharashtra, India
Dhananjay.sable165@gmail.com

Abstract: Outfitted with cutting edge Smartphone and cell phones, today's exceptionally interconnected urban populace is progressively reliant on these contraptions to sort out and arrangement their everyday lives. These applications frequently depend on current (or favored) areas of individual clients or a gathering of clients to give the sought administration, which imperils their security; clients would prefer essentially not to uncover their current (or preferred) locations to the administration supplier or to other, potentially untrusted, clients. In this paper, we propose protection saving calculations for deciding an ideal meeting area for a gathering of clients. We perform an intensive security assessment by formally measuring protection loss of the proposed methodologies. With a specific end goal to concentrate on the execution of our calculations in a genuine organization, we actualize and test their execution effectiveness. By method for a focused on client study, we endeavor to get an understanding into the protection familiarity with clients in area based administrations and the convenience of the proposed solutions.[1]

Keywords—*Mobile application, neglectful calculation, security.*

*****

1. INTRODUCTION

Location based system are gaining much important in many domain. Location privacy has become an important issue in such system. To solve this issue we have propose FRVP technique to improve in such systems. Gmaps are major resources for accessing location based services. A meeting location services is implemented to simulate privacy in location based system.

Two well-known elements of area based administrations are area registration and area sharing. By registering with an area, clients can impart their present area to family and companions or acquire area particular administrations from outsider suppliers. As per a late study, area sharing administrations are utilized by just about 20% of all cell telephone clients[1]. In this paper, we address the security issue in LSBSs by concentrating on a particular issue called the Fair Rendez-Vous Point (FRVP) issue. Given an arrangement of client area inclinations, the FRVP issue is to focus an area among the proposed ones such that the most extreme separation between this area and every single other client's areas is minimized, i.e. it is reasonable to all clients. We will probably give pragmatic protection saving strategies to tackle the FRVP issue, such that neither an outsider, nor partaking clients, can learn other clients' areas; taking an interest clients just take in the ideal area. The protection issue in the FRVP issue is illustrative of the applicable security dangers in LSBSs.

Our commitments in this paper are to create security arrangement alternatives for clients. To perform meeting area mapping with Google maps. To give client input choice. Giving area sharing administrations utilizing GMaps. We additionally address the multi-inclination case, where every client may have various organized area inclinations[3].

2. RELATED WORK

Igor Bilogrevic, proposed **1.** Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices. These applications often rely on current (or preferred) locations of individual users or a group of users to provide the desired service, which jeopardizes their privacy; users do not necessarily want to reveal their current locations to the service provider or to other, possibly untrusted, users. In this paper, we propose privacy-preserving algorithms for determining an optimal meeting location for a group of users[3]. We perform a thorough privacy evaluation by formally quantifying privacy-loss of the proposed approaches. In order to study the performance of our algorithms in a real deployment.[1]

2. This paper are actualize and test their execution effectiveness.[2]

E. Valavanis , proposed **3.** MobiShare: Sharing Context-Dependent Data & Services from Mobile Sources. cell phones that we use in regular life to wind up data and administrations suppliers by supplementing or supplanting settled area hosts associated with the wireline system. finding and getting to heterogeneous portable assets in an expansive zone, considering the connection of both sources and requestors[4].
M. Jadliwala , proposed **4.** Secure Distance-based Localization in the Presence of Cheating Beacon Nodes. This paper endeavors to locate a protected separation based area disclosure in vicinity of reference point hubs and confirm the precision and productivity of the analyses utilizing down to earth separation estimation mistake models[5].

3. PROPOSED SYSTEM

The proposed work is planned to be carried out in the following manner

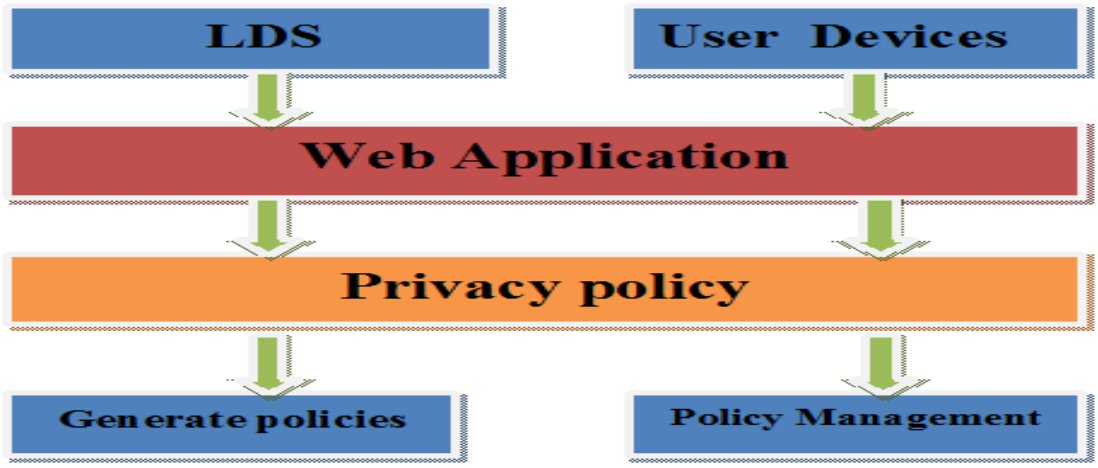

Fig.1: Basic system architecture.[3]

In this project privacy-preserving algorithms for determining an optimal meeting location for a group of users. We perform a thorough privacy evaluation by formally quantifying privacy-loss of the proposed approaches. In any Location-Sharing-Based Service (LSBS) is a major concern and must be addressed. Our goal is to provide practical privacy-preserving techniques to solve the FRVP(Fair Rendez-Vous Point) problem, such that neither a third-party, nor participating users, can learn other users' locations. In these architecture web application can determine the number of policies of user. Location Determination Server (LDS) can finding the location on user devices and provide a privacy policy on meeting location.[2]

Implementing the privacy policy for the user on meeting location. Provide the privacy to each user who get the meeting location. And we use the modified PPFRV(Privacy-Preserving Fair Rendz-Vous Point) algorithm. And also use the MD5 algorithm.

ALGORITHM:

PPFRVP:-
Algorithm privacy location (users user [ ], locations location [ ])
Step 1:- Read location of all users from location [ ]

For (i=0 to n-1)

Read Location [I] Into ARRAYLIST

End For

Step 2:- Perform reverse geocode using Gmap.

INITIALIZE GOOGLE API USING API KEY.

Google Map base = Gmap.Read Map

(www.googleapis.com);

Mapbase.connect (address, APIkey);

Step3:- Perform Transformation function.

$F = \sum_{i=0}^{n-1} L(f)$

Calculation:-

Initialize message digest on locations.

MD5 MessageDigest.initializehash();

ArrayList cipherlocation[ ]=MD5.

gethash(L(f));

Step 4:- Perform fairness function.

retrieveLoc r[ ]= User.getApprovedLocations(L(f));

Step 5:- Perform inverse transformation.

MD5 MessageDigest.initializehash( ).

Perform Inverse

$F = \sum_{i=0}^{n} L(f1)$

Step 6:- Perform fairness policy on all users.

$\sum_{i=0}^{n-1}$ fairness(f(l1));

Step 7:- Assign allotted location to all users.

$\sum_{i=0}^{n-1}$ multicast(L(f));

Step 8:- Stop.

JSON API

It is used to connect with google map. JSON API is a specification for how a client should request that resources be fetched or modified, and how a server should respond to those requests.

JSON API is designed to minimize both the number of requests and the amount of data transmitted between clients and servers. This efficiency is achieved without compromising readability, flexibility, or discoverability. JSON API require use of the JSON API media type application for exchanging data.[3]

Google Map service

Google maps allows you to display maps on your web application. Google maps API lets you customize maps, and the information on maps. An API is a set of methods and tools that can be used for building software application.

The google maps web services are a collection of HTTP interfaces to google services providing geographic data for your maps application. This guide service only to introduce the web service and host information common to all of the different services. Individual documentation for each service.

4. METHODOLOGY

4.1 Retrieve Locations

When using this application For retrieve location for meeting with the third party providers first we have to retrieve the location of the user.

4.2 Check User Location

Checking into a location, users can share their current location with family and friends or obtain location-specific services from third party providers. And also user can schedule their meeting by checking the other user locations.[3]

4.3 Schedule Meeting

After retrieving the location of the each user and checking location of the each user we can schedule the meeting on one specific space as per the users' convenience with date and time.

4.4 Check Meeting Status After schedule the meeting all users can send their opinion about meeting if they are able to attend the meeting by using approval or denied.

5. DESIGN WORK

The Design work is planned to be carried out in the following manner :

Firstly, implemented the new user registration to create the new user write the first name, last name, email id, and then upload the picture and then new user created successfully. Then the user one can retrieve location of the other user. The new user has to registration in the system. Then retrieve location for meeting from the other users and select the users for meeting and call them for the meeting.[3]

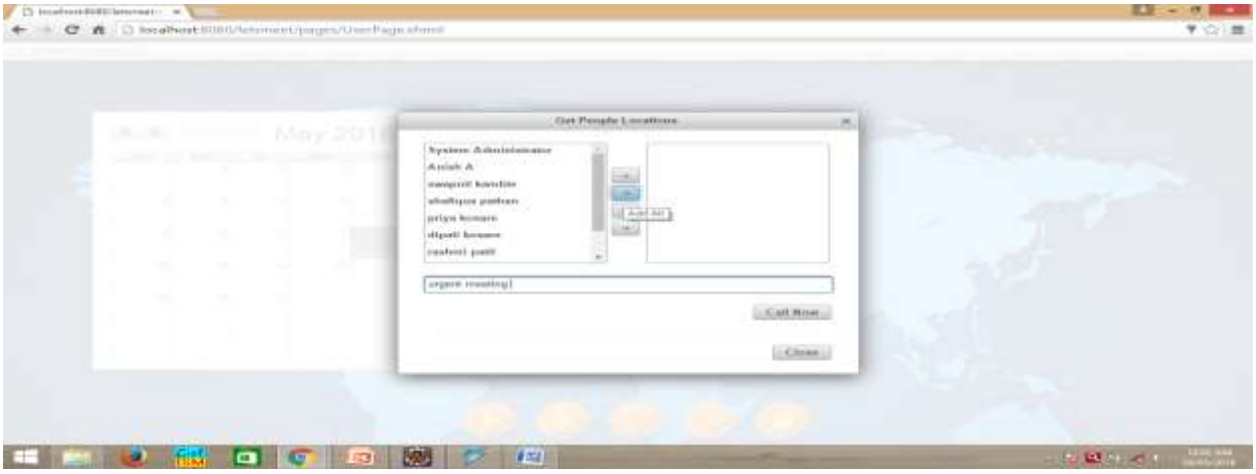

Fig 5.1 : Get people location

In above fig 5.1 shows the list of people to get the location of that people select the list to call for meeting then decide the title of the meeting and then call now. Then the user can send the request to the other list of users for retrieve the their location after sending the message to list of user then display the message get location request created successfully.

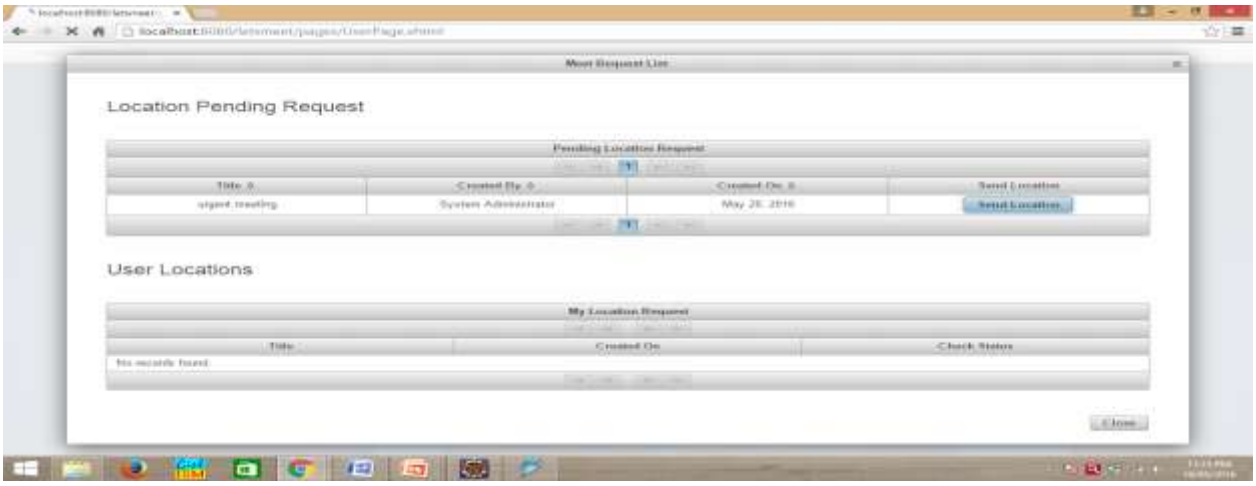

Fig 5.2 Send the location to whom user who sends location request

Secondly, Designed the check user location after sending the message to the list of users that user can get the message which contain the meeting title and the date & time and then they are send their location to that requester.

In above fig 5.2 shows send the location to whom users who send the location request then click on send location. Fig 5.3 To send the location to the user clicking on to the send location after that open the google map and choose the location and then send to the users.

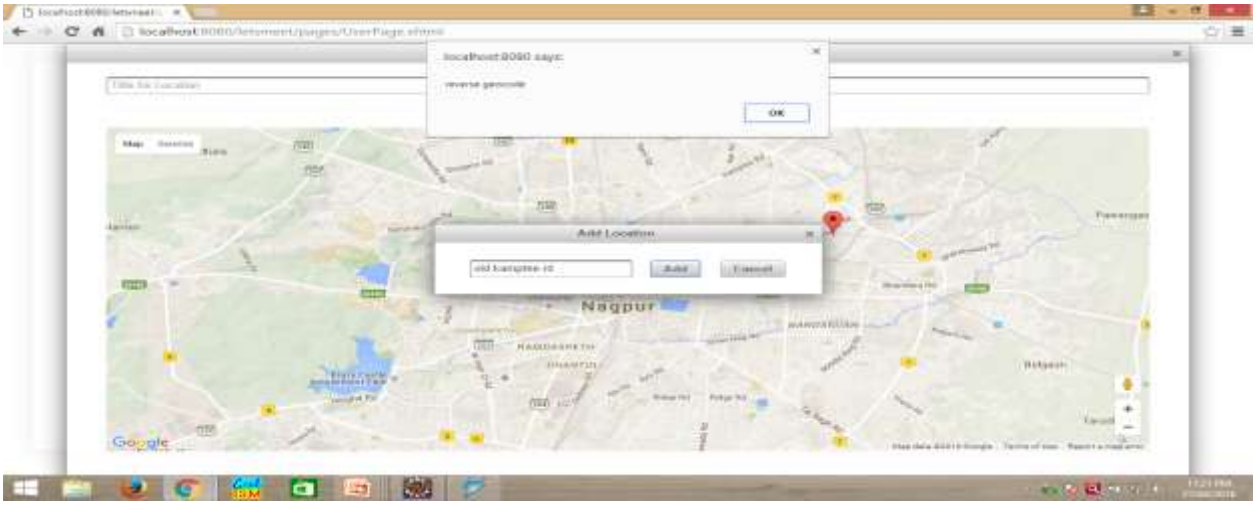

Fig 5.3: Sending the Location by using google map

Thirdly, designed the schedule meeting after user can get the location of the list of users then the user can schedule the location that is convenient to each and every users and also schedule the date and time of the meeting.

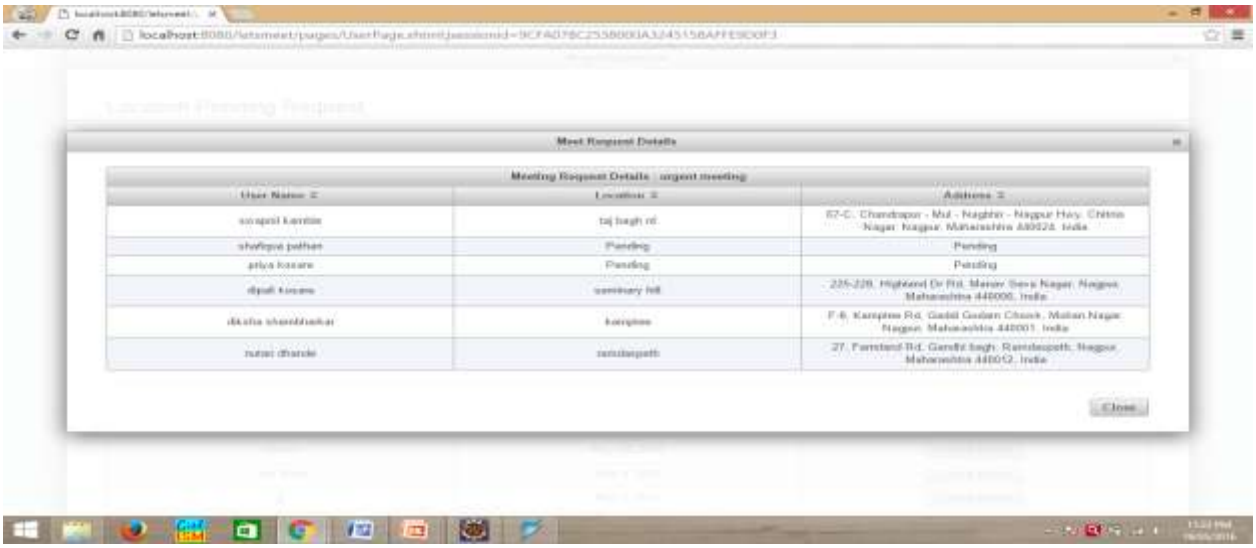

Fig 5.4: Meeting request detail

Fig 5.5: schedule meeting location

Fig 5.4 shows the meeting requests detail that consist of the list of person who send their location who get message for meeting request. Fig. 5.5 after the getting the location of list of users then schedule meeting location by using google map to fix particular location for meeting. Then the schedule meeting it contain the title of meeting and place of the meeting location and list of users who are invited for the meeting and also date and time of meeting and then send to the users who are invited and then meeting is schedule meeting is fixed. After that meeting created successfully.

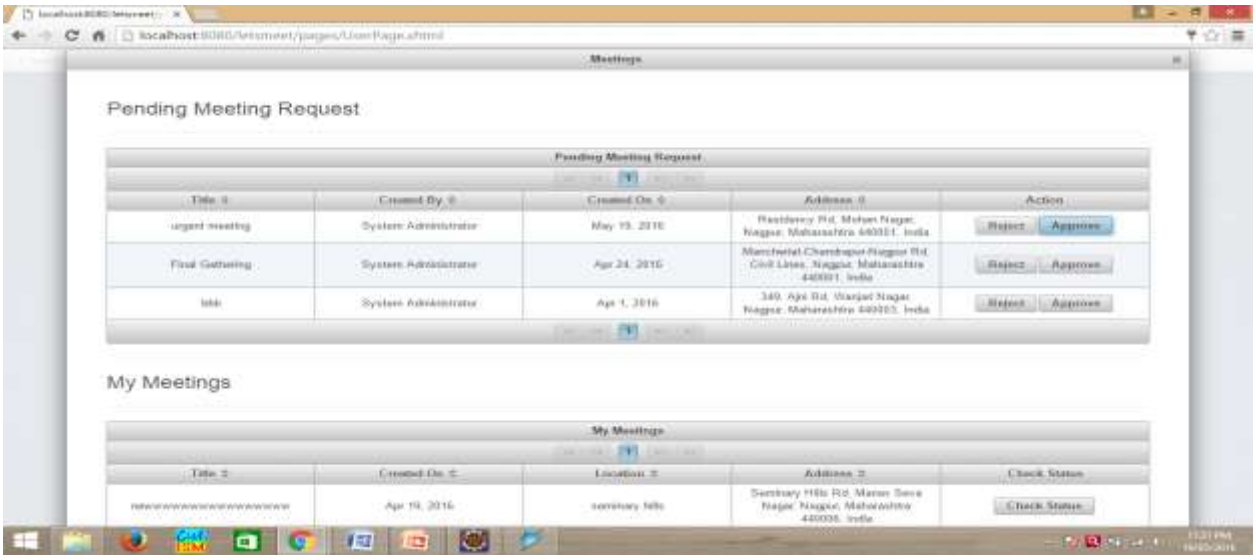

Fig. 5.6 Approve or Reject meeting

Fourthly, designed the check meeting status it can be check the meeting status that is user can send if the user can convenient with the location then user can send their opinion about meeting if they are possible to attend the meeting user can approve or denied. Fig 5.6 shows the meeting request which contain the meeting request from the other user if it is possible to attend the meeting then approve or denied. if the list of user can approve the meeting request then the optimal meeting is successfully created

6. RESULT

1. Broadcasting request

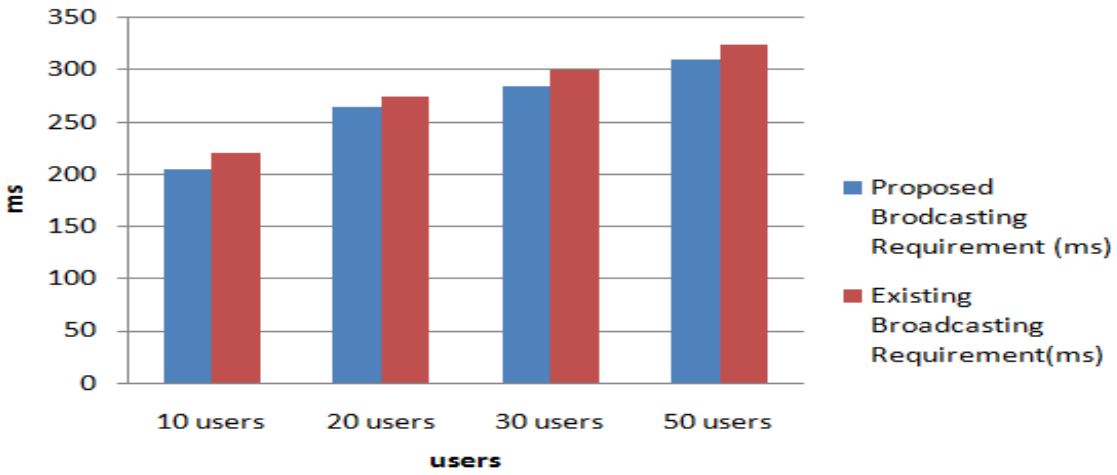

Fig. 8.1: Broadcasting requirement

In above fig. shows the result time in millisecond for broadcasting request for the number of users.

2. Location Retrieval Gmap

Fig. 8.2 Location retrieval Gmap

In above fig.8.2 shows the 2 mbps upto 256kbps Gmap can load in few millisecond.

3. Time Required

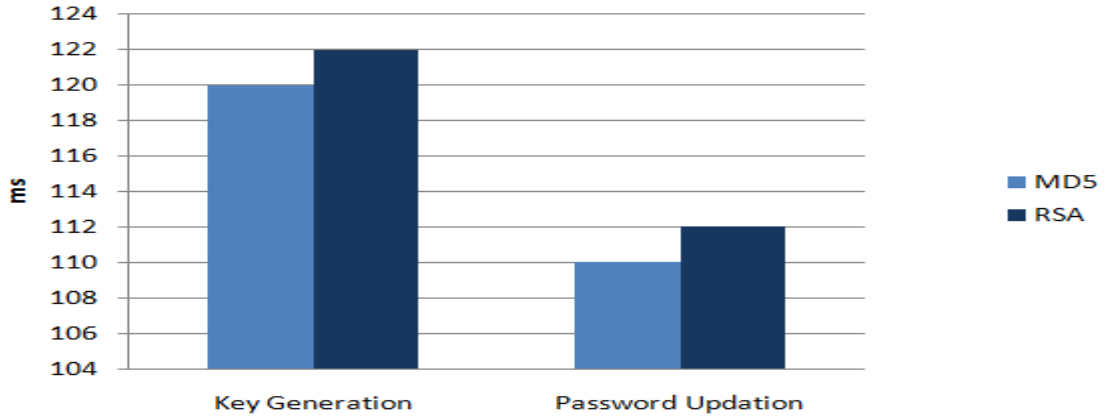

Fig. 8.3 Time required

In above fig. 8.3 shows the result of time required in millisecond for key generation and password generation.

4. Comparatively Analysis

In bellows fig. 8.4 shows the comparatively analysis result in between the algorithm of BGN160, BGN256,ELGPAL and Proposed required time in millisecond of each algorithm.

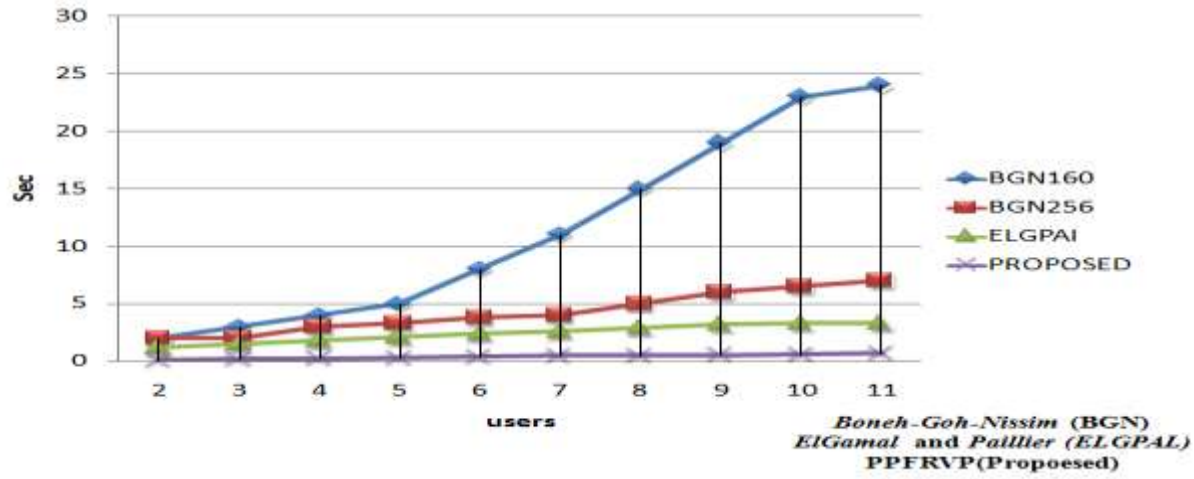

Fig. 8.4: Comparatively Analysis

7. CONCLUSION

In resent year location based service have gained importance due to fast internet connectivity services and location determination service provided by different service provider. Due to this user location privacy issues has arise to secure a user location from another user. At the same time user privacy maintenance has become harder in group user services like meeting arrangement.

In this project proposed a fair policy protocol where user privacy is important and transparency mechanism is implement between group of user location sharing system.

In this project used JSON API for accessing Gmap (a google provided location fetch system) from result we can verify that proposed framework provider better privacy in sharing user location system.

8. FUTURE SCOPE

Make system compatible for IOS system so easily location can be retrieved. We also plan to lower down the time require to access data from Google using new update API.

REFERENCESS

[1] Igor Bilogrevic, Member, IEEE, Murtuza Jadliwala, Member, IEEE, Vishal Joneja, Kübra Kalkan, Jean-Pierre Hubaux, Fellow, IEEE, and Imad Aad "*Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices*", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 7, JULY 2014.

[2] [1]Dipali D. Kosare, [2]Prof. D. M. Sable,"A Survey paper on Optimal Confrontation Location Decision Based on User Privacy", International Journal of Research (IJR) e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015.

[3] [1]Dipali D. Kosare, [2]Prof. D. M. Sable, [3]Prof. D. S. Dabhade," Optimal Confrontation Location Decision Based on User Privacy", IJRITCC ISSN: 2321-8169 Volume: 4 Issue : 1 14 – 19 January 2016**.**

[4] E. Valavanis, C. Ververidis, M. Vazirgianis, G. C. Polyzos, and K. Norvag, ―MobiShare: Sharing context-dependent data & services from mobile sources,‖ in Proc. IEEE/WIC Int. Conf. WI, Oct. 2003, pp. 263–270.

[5] M. Jadliwala, S. Zhong, S. J. Upadhyaya, C. Qiao, and J.-P. Hubaux, "Secure distance-based localization in the presence of cheating beacon nodes," IEEE Trans. Mobile Comput., vol. 9, no. 6, pp. 810– 823, Jun. 2010.

[6] C. Zhang and Y. Huang, ―Cloaking locations for anonymous location based services,‖ GeoInformatica, vol. 13, no. 2, pp. 159–182, 2009

[7] P. Santos and H. Vaughn, ―Where shall we meet? Proposing optimal locations for meetings,‖ in Proc. MapISNet, 2007.

[8] F. Berger, R. Klein, D. Nussbaum, J.-R. Sack, and J. Yi, ―A meeting scheduling problem respecting time and space,‖ GeoInformatica, vol. 13, no. 4, pp. 453–481, 2009.
[9] C. Ardagna, M. Cremonini, E. Damiani, S. Vimercati, and P. Samarati, ―Location privacy protection through obfuscation-based techniques,‖ in Proc. 21st IFIP WG 11.3 Working Conf. Data and Applications Security, 2007.
[10] Zhong, I. Goldberg, and U. Hengartner, ―Louis, Lester and Pierre: Three protocols for locationprivacy,‖ in Proc. 7th Int. Conf. Privacy Enhancing Technologies, 2007, pp. 62–76.
[11] A. Solanas and A. Martínez-Ballesté, ―Privacy protection in locationbased services through a public-key privacy homomorphism,‖ in Proc. 4th European Conf. Public Key Infrastructure, Theory and Practice, 2007, pp. 362–368.
[12] C.-H. O. Chen et al., ―GAnGS: Gather, authenticate ’n group securely,‖ in Proc. 14th ACM Int. Conf. Mobile Computing Networking, 2008, pp. 92–103.
[13] J. Krumm, ―A survey of computational location privacy,‖ Personal Ubiquitous Comput., vol. 13, no. 6, pp. 391–399, 2009.
[14] J. Freudiger, M. Jadliwala, J.-P. Hubaux, V. Niemi, P. Ginzboorg, and I. Aad, ―Privacy of community pseudonyms in wireless peer-to- peer networks,‖ Mobile Netw. Appl., vol. 18, no. 3, pp. 413–428, 2012.
[15] R. Rivest, A. Shamir, and L. Adleman, ―A method for obtaining digital signatures and public-key cryptosystems,‖ Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.
[16] B. Gedik and L. Liu, ―Location privacy in mobile systems: A personalized anonymization model,‖ in Proc. 25th IEEE ICDCS, Jun. 2005, pp. 620–629.
[17] S. Pidcock and U. Hengartner, ―Zerosquare: A privacy-friendly location hub for geosocial applications,‖ in Proc. 2nd ACM SIGCOMM Workshop Networking, Systems, and Applications Mobile Handhelds, 2013.
[18] S. Guha, M. Jain, and V. Padmanabhan, ―Koi: A location-privacy splatform for smartphone apps,‖ in Proc. 9th USENIX Conf. NSDI, 2012.
[19] M. Herrmann, A. Rial, C. Diaz, and B. Preneel, ―Privacy-preserving location-sharing-based services,‖ COSIC, Katholieke Univ. Leuven, Leuven, Belgium, Tech. Rep., 2013.
[20] B. Carbunar, R. Sion, R. Potharaju, and M. Ehsan, ―The shy mayor: Private badges in geosocial networks,‖ in Proc. 10th Int. Conf. ACNS, 2012, pp. 436–454.
[21] K. B. Frikken and M. J. Atallah, “Privacy preserving route planning,‖ in Proc. ACM WPES, 2004, pp. 8–15.
[22] P. Golle and K. Partridge, ―On the anonymity of home/work location pairs‖,in Proc. 7th Int. Conf. Pervasive Computing, 2009, pp. 390– 397
[23] J. Freudiger, R. Shokri, and J.-P. Hubaux, “Evaluating the privacy risk of location-based services,” in Proc. 15th Int. Conf. Financial, 2011, pp. 31–46.
[24] V. Vazirani, *Approximation Algorithms*. New York, NY, USA: Springer-Verlag, 2001.
[25] I. Bilogrevic, M. Jadliwala, K. Kalkan, J. Hubaux, and I. Aad, “Privacy in mobile computing for location-sharing-based services,” in *Proc. 11th Int. Conf. PETS*, 2011, pp. 77 96.
[26] (2011, Nov.). *UTM Coordinate System* [Online]. Available: https://www.e-education.psu.edu/natureofgeoinfo/c2_p21.html
[27] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. Tan, “Private queries in location based services: Anonymizers are not necessary,” in *Proc. ACM SIGMOD*, 2008, pp. 121–132.
[28] M. Jadliwala, S. Zhong, S. J. Upadhyaya, C. Qiao, and J.-P. Hubaux, “Secure distance-based localization in the presence of cheating beacon nodes,” *IEEE Trans. Mobile Comput.*, vol. 9, no. 6, pp. 810–823, Jun. 2010.
[29] C.-H. O. Chen *et al.*, “GAnGS: Gather, authenticate ’n group securely,” in *Proc. 14th ACM Int. Conf. Mobile Computing Networking*, 2008, pp. 92–103.